ISM LAB 2

<div align="right">

SANTHOSH KRISHNA R

21BCE1651

</div>

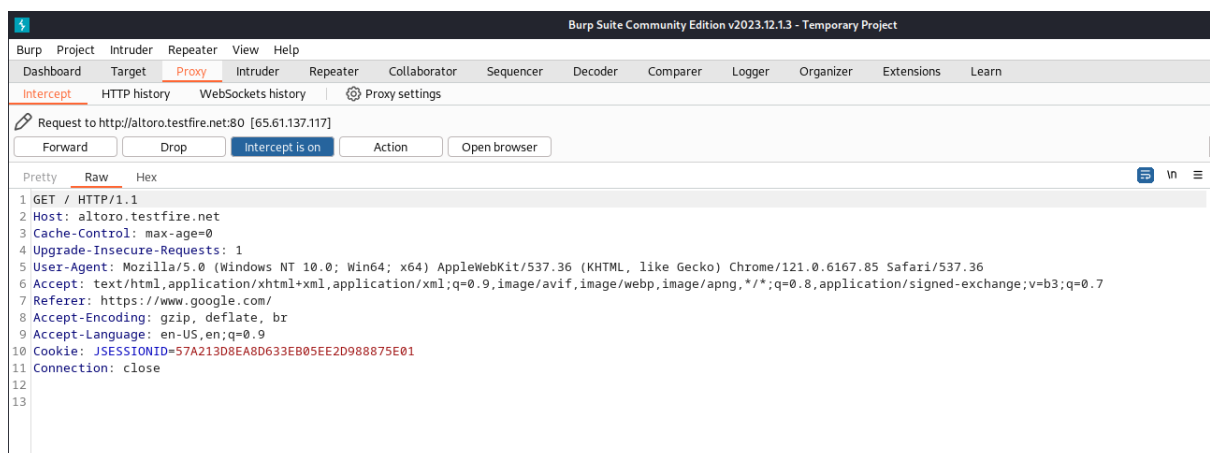**Aim:** To use Burp Suite to conduct brute force attack.

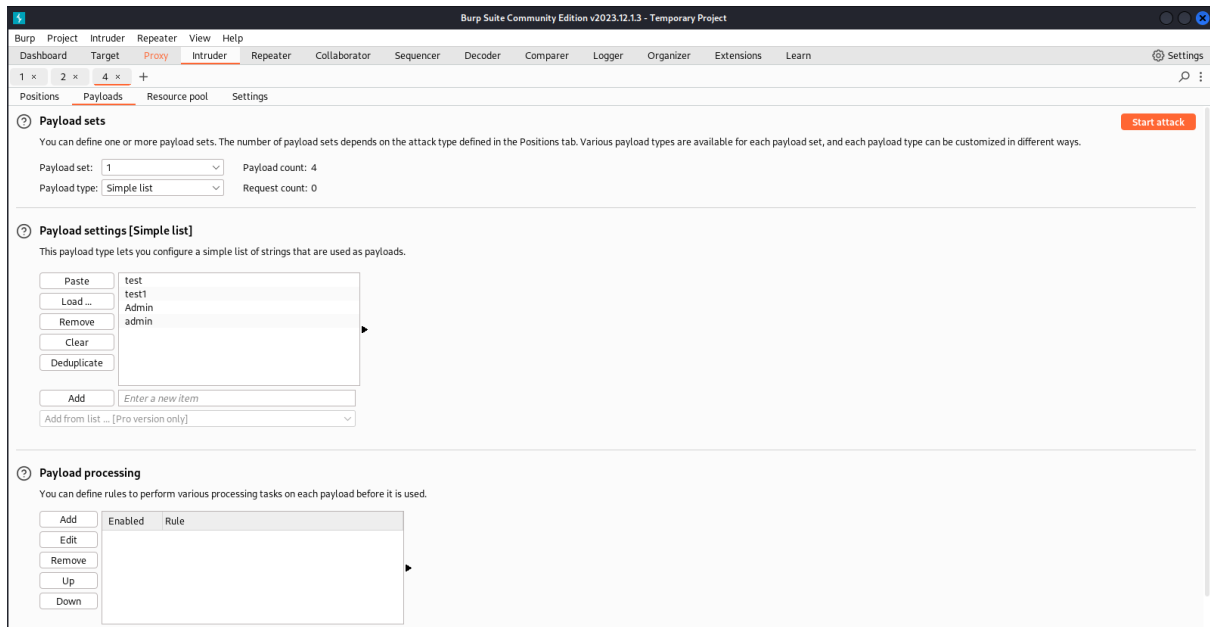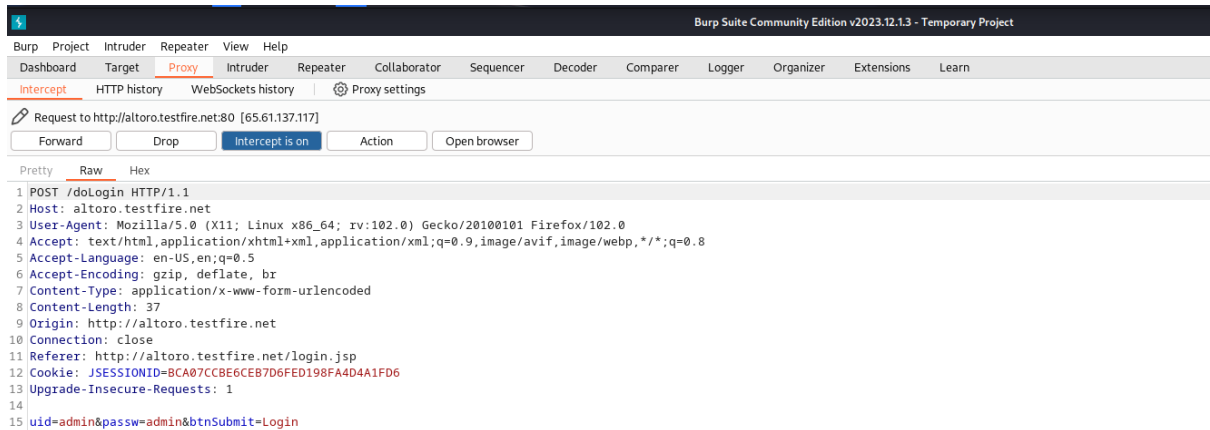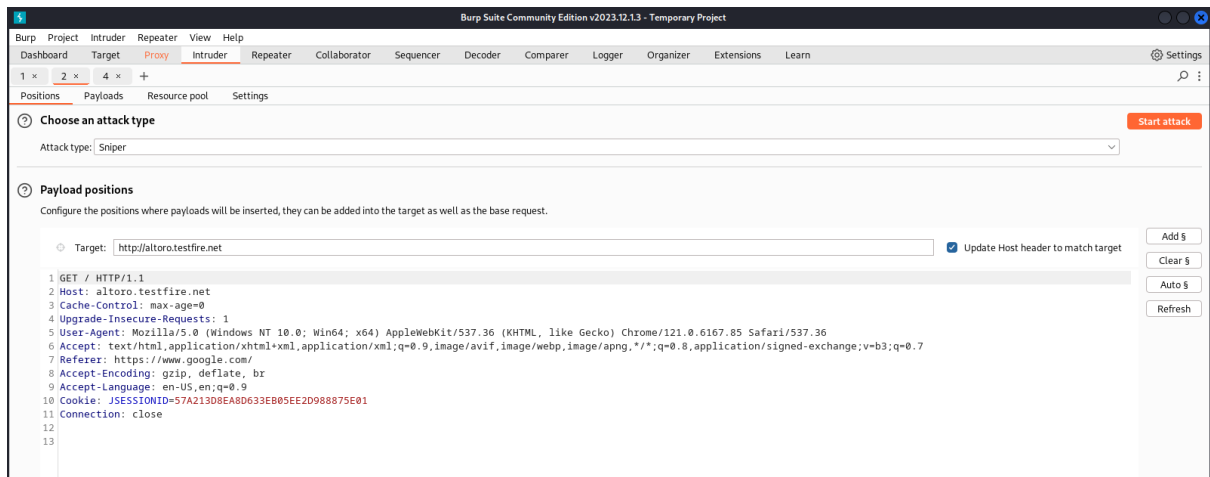**Apparatus Required:** Burp Suite, Foxy Proxy

Theory & Commands involved:

Brute Force: A brute force attack uses trial-and-error to guess login info, encryption keys, or find a hidden web page. It plays a vital role in web penetration testing because is the simplest method to gain access to a site or server by checking the correct username or password by calculating every possible combination that could generate a username or password.

Brute Force in Burp Suite using Intruder: Burp Suite is a set of tools used for penetration testing of web applications. Burp Intruder is a tool for automating customized attacks against web applications. The intruder is used for Brute-force attacks on password forms, pin forms, and other such forms. Burp Intruder supports various attack types - these determine the way in which payloads are assigned to payload positions.

Screenshots:

Burp Project Intruder Repeater View Help

Dashboard   Target   Proxy   Intruder   Repeater   Collaborator   Sequencer   Decoder   Comparer   Logger   Organizer   Extensions   Learn   Settings

1 ×   2 ×   4 ×   +

Positions   Payloads   Resource pool   Settings

Choose an attack type   Start attack

Attack type: Sniper   ▼

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://altoro.testfire.net   ☑ Update Host header to match target   Add §
                                                                                                                                                                                            Clear §
```
1 GET / HTTP/1.1
2 Host: altoro.testfire.net
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Referer: https://www.google.com/
8 Accept-Encoding: gzip, deflate, br
9 Accept-Language: en-US,en;q=0.9
10 Cookie: JSESSIONID=57A213D8EA8D633EB05EE2D988875E01
11 Connection: close
12
13
```
                                                                                                                                                                                            Auto §
                                                                                                                                                                                            Refresh

---

Burp Project Intruder Repeater View Help

Dashboard   Target   Proxy   Intruder   Repeater   Collaborator   Sequencer   Decoder   Comparer   Logger   Organizer   Extensions   Learn

Intercept   HTTP history   WebSockets history   Proxy settings

✎ Request to http://altoro.testfire.net:80 [65.61.137.117]

Forward   Drop   Intercept is on   Action   Open browser

Pretty   Raw   Hex

```
1 POST /doLogin HTTP/1.1
2 Host: altoro.testfire.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 37
9 Origin: http://altoro.testfire.net
10 Connection: close
11 Referer: http://altoro.testfire.net/login.jsp
12 Cookie: JSESSIONID=BCA07CCBE6CEB7D6FED198FA4D4A1FD6
13 Upgrade-Insecure-Requests: 1
14
15 uid=admin&passw=admin&btnSubmit=Login
```

Burp Project Intruder Repeater View Help

Dashboard   Target   Proxy   Intruder   Repeater   Collaborator   Sequencer   Decoder   Comparer   Logger   Organizer   Extensions   Learn   Settings

1 ×   2 ×   4 ×   +

Positions   Payloads   Resource pool   Settings

Payload sets   Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 ▼   Payload count: 4
Payload type: Simple list ▼   Request count: 0

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste   test
Load ...   test1
Remove   Admin
Clear   admin
Deduplicate

Add   Enter a new item
Add from list ... [Pro version only]   ▼

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add   Enabled   Rule
Edit
Remove
Up
Down

Attack   Save   Columns

2. Intruder attack of http://localhost:80

Attack ∨   Save ∨   Columns ∨

Results   Positions   Payloads   Resource pool   Settings

Filter: Showing all items

Request	Position	Payload	Status code	Error	Timeout	Length	Comment
0				☑	☐		
1	1	admin		☑	☐		
2	1	Admin		☑	☐		
3	1	test1		☑	☐		
4	1	test		☑	☐		
5	2	admin		☑	☐		
6	2	Admin		☑	☐		
7	2	test1		☑	☐		
8	2	test		☑	☐		
9	3	admin		☑	☐		
10	3	Admin		☑	☐		
11	3	test1		☑	☐		
12	3	test		☑	☐		

Altoro Mutual   ✕   +

← → C ⌂   ○ 🔒 altoro.testfire.net/bank/main.jsp   📄 ☆   ♥   burp   ≡

🐉 Kali Linux   🐲 Kali Tools   📄 Kali Docs   🐉 Kali Forums   🦎 Kali NetHunter   🔥 Exploit-DB   🐝 Google Hacking DB   ⦿ OffSec

AltoroMutual

Sign Off | Contact Us | Feedback | Search [   ] Go

| MY ACCOUNT | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL |

I WANT TO ...
- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION
- Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: [800000 Corporate ∨]   GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

Click Here to apply.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2024 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features